



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/388,388	09/01/1999	FUMIHIKO SANO	04329.2163	3921

22852 7590 08/05/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER

BAUM, RONALD

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 08/05/2003

8

Please find below and/or attached an Office communication concerning this application or proceeding.

14

Office Action Summary

Application No.

09/388,388

Applicant(s)

SANO ET AL.

Examiner

Ronald Baum

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☒ Claim(s) 10-13 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5,6,7.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: .

DETAILED ACTION

1. Claims 1-13 are pending for examination.
2. Claims 1-9 are rejected.
3. Claims 10-13 are objected to.

Priority

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1,2,8 are rejected under 35 U.S.C. 102(b) as being anticipated by Coppersmith et al, U.S. Patent 5,768,390.

4. As per claim 1 ; “An encryption/decryption unit for encrypting a plaintext into a ciphertext and/or decrypting a ciphertext into a plaintext [col. 3, lines 29-47, line 13, col. 8, lines 10- 16, figure 2 (& col. 4, lines 54- col.5, line 25)], comprising: first encryption/decryption means for performing an encryption or decryption process [col. 3, lines 33-35]; first substitution means for performing data substitution of an output from said first encryption/ decryption means according to a predetermined permutation table [col. 3, lines 33-35]; second encryption/decryption means for performing an encryption or decryption process for an output

Art Unit: 2131

from said first substitution means [col. 3, lines 39-43]; second substitution means for performing data substitution of an output from said second encryption/decryption means according to a predetermined permutation table [col. 3, lines 39-43]; and third encryption/decryption means for performing an encryption or decryption process for an output from said second substitution means [col. 3, lines 43-46].” ;

And further as per claim 8 ; “A computer-readable storage medium storing a program [This claim is the software embodiment of the method claim 1, and is rejected for the same reasons provided for the claim 1 rejection above] for controlling an encryption/decryption unit for encrypting a plaintext into a ciphertext and/or decrypting a ciphertext into a plaintext, the program comprising: first encryption/decryption means for performing an encryption or decryption process; first substitution means for performing data substitution of an output from said first encryption/decryption means according to a predetermined permutation table; second encryption/decryption means for performing an encryption or decryption process for an output from said first substitution means; second substitution means for performing data substitution of an output from said second encryption/decryption means according to a predetermined permutation table; and third encryption/decryption means for performing an encryption or decryption process for an output from said second substitution means.” ;

5. Claim 2 *additionally recites* the limitations that “A unit according to claim 1, wherein said first encryption/decryption means, said third encryption/decryption means, said first substitution means, and said second substitution means are means which comply with the same algorithm.”. The teachings of Coppersmith et al (col. 3, lines 58- col. 4, line 13, col. 8, lines 10-16,) suggest such limitations (i.e., DES algorithmically based);

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 3-7, 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al, U.S. Patent 5,768,390, and further in view of Coppersmith et al, U.S. Patent 5,454,039.

6. As per claim 3 ; “A unit according to claim 1, wherein said unit further comprises key generating means for generating intermediate keys respectively supplied to said first, second, and third encryption/decryption means ” ;

Coppersmith et al, U.S. Patent 5,768,390 teaches of the multi stage DES encryption with inter-encryption processing (i.e., substitution means).

Coppersmith et al, U.S. Patent 5,768,390 fails to teach of the intermediate key generation used for the various encryption/ decryption and substitution processing sections being generated on the unit.

Coppersmith et al, U.S. Patent 5,454,039 teaches of using an encryption key to generate a indexed table of pseudorandom values (i.e., intermediate key values used for encryption/ decryption unit processing).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Coppersmith et al, U.S. Patent 5,768,390 teaches of the multi stage DES encryption with the Coppersmith et al, U.S. Patent 5,454,039 teaches of using an encryption key to generate a indexed table of pseudorandom values for speeding up the encryption of the Coppersmith et al, U.S. Patent 5,768,390 multi stage DES encryption in that by the serial nature of multi stage encryption, more time is required such that this is where speed optimization via key or pre key (i.e., pseudorandom values) pre processing would be an advantage (Coppersmith et al, U.S. Patent 5,454,039, col. 1, lines 13-50).

Further, as per claim 3; “[and] said first and second substitution means, and said first and second substitution means function as identity conversion when the intermediate key generated by said key generating means contains predetermined data.” ; The teachings of Coppersmith et al, U.S. Patent 5,768,390 (col. 3, lines 58- col. 4, line 13) suggest such limitations (i.e., the mask configured with DES with a key predetermined to cause DES ciphertext output to equal the plaintext input, such as a key of all zeros);

7. And further, claim 9 ***additionally recites*** the limitations that “A medium [This claim is the software embodiment of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above] according to claim 8, wherein said medium further comprises key generating means for generating intermediate keys respectively supplied to said first, second, and third encryption/decryption means and said first and second substitution means, and said first and second substitution means function as identity conversion when the intermediate key generated by said key generating means contains predetermined data.” [This claim is the

Art Unit: 2131

apparatus of the method claim 3, and is rejected for the same reasons provided for the claim 3 rejection above];

8. Claim 4 ***additionally recites*** the limitations that “A unit according to claim 3, wherein said first and third encryption/decryption means are means which comply with the same algorithm as that for said second encryption/decryption means when the intermediate key generated by said key generating means contains predetermined data.” ; The teachings of Coppersmith et al, U.S. Patent 5,768,390 (col. 3, lines 58- col. 4, line 13, col. 8, lines 10- 16, figure 2 (& col. 4, lines 54- col.5, line 25)) suggest such limitations (i.e., the encryption/decryption unit and the mask configured with DES with a key predetermined to cause DES ciphertext output to equal the plaintext input, such as a key of all zeros).

9. Claim 5 ***additionally recites*** the limitations that “A unit according to claim 3, wherein said second encryption/decryption means executes a decryption process when said first and third encryption/decryption means perform an encryption process, and executes an encryption process when said first and third encryption/decryption means executes a decryption process.” ; The teachings of Coppersmith et al, U.S. Patent 5,768,390 (col. 3, lines 58- col. 4, line 13, col. 8, lines 10- 16, figure 2 (& col. 4, lines 54- col.5, line 25)) suggest such limitations (i.e., the encryption/ decryption units configured for basic triple DES, and the mask configured with DES with a key predetermined to cause DES ciphertext output to equal the plaintext input, such as a key of all zeros).

10. Claim 6 ***additionally recites*** the limitations that “A unit according to claim 5, wherein said key generating means supplies the same intermediate key to said first and third encryption/decryption means.” ; The teachings of Coppersmith et al, U.S. Patent 5,768,390 (col.

Art Unit: 2131

3, lines 50- col. 4, line 13, col. 8, lines 10- 16, figure 2 (& col. 4, lines 54- col.5, line 25)) suggest such limitations (i.e., the encryption/ decryption units configured for basic triple DES with 2 keys (triple DES in $E[k_1]D[k_2]E[k_1]$ mode), and the mask configured with DES with a key predetermined to cause DES ciphertext output to equal the plaintext input, such as a key of all zeros).

11. Claim 7 *additionally recites* the limitations that “A unit according to claim 5, wherein said key generating means supplies intermediate keys that cause said first and second encryption/decryption means or said second and third encryption/decryption means to comply with the same algorithm and use the same encryption/decryption key. ” ; The teachings of Coppersmith et al, U.S. Patent 5,768,390 (col. 3, lines 50- col. 4, line 13, col. 8, lines 10- 16, figure 2 (& col. 4, lines 54- col.5, line 25)) suggest such limitations.

Allowable Subject Matter

12. Claim 10 *additionally recites* the limitations that “A unit according to claim 3, wherein said key generating means comprises: dividing means for dividing key data K of a predetermined number of bits into a plurality of data and storing the divided data into respective registers; expanded permutation means for reading out the divided key data from the respective registers and effecting an expanded permutation on the divided key data; DES-SS key schedule means for generating intermediate keys K1 and K3 from a result of the expanded permutation performed by said expanded permutation means [Prior art of record is silent on the claim element and any motivation to combine the above claim element.]; DES key schedule means for generating an intermediate key K2 from a result of the expanded permutation performed by said expanded

Art Unit: 2131

permutation means; and substitution schedule means for generating intermediate keys KK1 and KK2 from the contents of the registers. ” ;

Claim 10 is objected to as being dependent upon a rejected base claim (claim 3), but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims:

13. Claim 11 *additionally recites* the limitations that “A unit according to claim 10, wherein said expanded permutation means comprises--an expanded permutation table for expanding input 56-bit key data into 64-bit data. ” ;

Claim 11 is objected to as being dependent upon a rejected base claim (claim 3), but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

14. Claim 12 *additionally recites* the limitations that “A unit according to claim 10, wherein said substitution schedule means receives one of the divided key data as a 32-bit key, and outputs an intermediate key KK1 input to said first substitution means and an intermediate key KK2 input to said second substitution means, said substitution schedule means comprising: first means for directly outputting the input 32-bit key as an intermediate key KD1 of said first substitution means, calculating a logical OR of the intermediate key, and outputting the logical OR as an intermediate key KS1 (one bit) of said first substitution means; and second means for shifting the input 32-bit key to the left to output the key as an intermediate key KD2 of said second substitution means, and calculating a logical OR of the intermediate key KD2 to output the key as an intermediate key KS2 (one bit) of said second substitution means. ” ;

Art Unit: 2131

Claim 12 is objected to as being dependent upon a rejected base claim (claim 3), but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. Claim 13 *additionally recites* the limitations that “A unit according to claim 12, wherein each of said first and second substitution means comprises an initial permutation section, an exclusive OR, a substitution portion, and an inverse permutation section, and said initial permutation section performs bit permutation of a 64-bit input and divides the permutation result into 8 blocks each comprising 8 bits, 32-bit data comprised of the first four 8-bit blocks of the output of said initial permutation section are directly input to said substitution portion, and 32-bit data comprised of the remaining four blocks is exclusive-ORed with the intermediate key KD, and a result of the exclusive-OR operation is output to said substitution portion, said substitution portion outputs output data corresponding to an input using a permutation table when the 1-bit key KS is at “1”, and outputs data identical to the input when the 1-bit key KS is at “0”, and said inverse permutation section receives the output data from said substitution portion, performs bit permutation of the received data, and outputs the data as 64-bit data. ” ;

Claim 13 is objected to as being dependent upon a rejected base claim (claim 3), but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 2131

1. Van Rumpt et al U.S. Patent 5,231,662
2. Becker U.S. Patent 4,157,454
3. Garcken et al U.S. Patent 5,778,074
4. Ohmori et al. U.S. Patent 6,570,989
5. Ritter U.S. Patent 5,623,549
6. Sprunk et al U.S. Patent 5,606,616
7. Akiyama et al U.S. Patent 5,623,548

17. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:


After-final (703) 746-7238

Official (703) 746-7239

Non-Official/Draft (703) 746-7246

Ronald Baum

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100